

# IDOR (Insecure Direct Object Reference)

IDOR (Insecure direct object references )

`https://example.com/?id=2`

`DELETE /file=ahmed.txt => ali.txt`

- ال IDOR هيا انك تقدر توصل لحاجات مش مسموح ليك انك توصلها
- مثلا انت ف ملف اسمو YYYY.txt بيظهر ف الرابط ال Path لو انت غيرته قدرت توصل لملف ثاني تبقي كذا في IDOR
- او لو انت مثلا ليك ID ف الموقع 123 واللي بعدك ليه 124 وهكذا لو انت غيرت ال ID بتاعك ل 124 و قدرت توصل ليه تبقي كذا IDOR

## Note

- تخيل إنك داخل على موقع بنك، وده رابط كشف حسابك:

`https://bank.com/account?user_id=1234`

فانت رقمك كمستخدم هو 1234، والموقع بيعرض بياناتك بناءً على الرقم ده.

لكن تخيل لو أي حد غيرك غير الرقم ده في الرابط كده:

`https://bank.com/account?user_id=1235`

وفجأة ظهرت له بيانات شخص ثاني!

كده الموقع مصاب بثغرة IDOR، لأنه ما تحققش هل المستخدم اللي طالب البيانات فعلاً عنده الحق يشوفها.

`https://example.com?username=mohamed => chat mohamed`

- مش ID بس ممكن تغيير ف اسم ال USER برضو

```

Pretty Raw Hex
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0aa10038034049ee81f6ea12007c00d8.web-security-academy.net
3 Cookie: session=I9Q9SGt1Uwy8mvnU8kai321MuLtyT3bU; Admin=false
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa10038034049ee81f6ea12007c00d8.web-security-academy.net/admin
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17

```

- ممكن تحاول تخش ك admin وتوقف الطلب وتغير ال True ل False
- هتبقى ادمن ومعاك صلاحيات اعلي

```

1 => username=ahmed    => id=1002
2 => username=hacker    => id=1003

```

- وانت بتعمل الثغره دي علشان تجربها انت تعمل اكونتين
- وبتعرف ال id وكل حاجه
- تخش علي ال burp وتحلل ال Requets وتشوف لقيتو بيرجعك ال username غيره باسم الاكونت الثاني
- لقيتو بيرجع ال id حط id الاكونت الثاني